Clause de non-responsabilité

Avertissement juridique

Ce guide et son contenu (le « Guide ») sont fournis par NXGEN. Tous les droits sur le Guide et sur la propriété intellectuelle qu'il incorpore — y compris, sans s'y limiter, les marques, noms commerciaux, logos et signes similaires figurant dans ou sur le Guide — sont protégés par la loi. L'ensemble des droits, titres et intérêts relatifs au Guide et aux droits de propriété intellectuelle qui s'y rapportent appartiennent et demeurent à NXGEN et à ses concédants.

Le Guide est fourni gratuitement, « en l'état » et à titre d'information uniquement, sans garantie d'aucune sorte. Il n'est ni destiné ni propre à établir une quelconque relation juridique entre le lecteur et NXGEN ou ses sociétés affiliées, y compris, sans s'y limiter, une quelconque obligation de NXGEN ou de ses sociétés affiliées envers le lecteur.

Les obligations de NXGEN et de ses sociétés affiliées concernant les produits ou services NXGEN achetés par un client sont régies exclusivement par les termes du contrat au titre duquel ces produits ou services ont été achetés.

Pour clarification

Le lecteur assume l'intégralité du risque quant à l'utilisation, aux résultats et aux performances du Guide. Dans toute la mesure permise par la loi applicable, NXGEN décline et exclut toutes garanties, qu'elles soient légales, expresses ou implicites — y compris, sans s'y limiter, les garanties implicites de qualité marchande, d'adéquation à un usage particulier, de titre et de non-contrefaçon des droits de tiers — ainsi que toute responsabilité ou garantie découlant de suggestions, spécifications ou échantillons liés au Guide.

Rôles et permissions

Updated 16 August 2026

Ce que fait le RBAC

Le Contrôle d'Accès Basé sur les Rôles (RBAC) dans GCXONE offre aux administrateurs un contrôle granulaire sur ce que les utilisateurs peuvent faire et sur les entités qu'ils peuvent voir.

> Distinction clé : Accès à l'Entité vs. Privilèges
>
> L'accès à l'entité et les privilèges sont des concepts distincts dans GCXONE. Les privilèges (configurés dans le rôle) déterminent QUELLES actions un utilisateur peut effectuer. L'accès à l'entité détermine QUELS clients, sites, appareils et capteurs ils peuvent voir. La personnalisation au niveau utilisateur se fait uniquement par l'accès à l'entité — il n'y a pas de dérogations de privilèges au niveau utilisateur.

Pourquoi c'est important

- « Je dois sauter entre plusieurs pages pour voir quel accès un poste offre réellement »
- « Créer un nouveau rôle prend une éternité avec trop d'étapes de configuration »
- « Je ne peux pas rapidement déterminer quelles permissions ont mes utilisateurs »
- « Deux utilisateurs dans le même rôle ont besoin d'accéder à des clients différents, mais je dois créer des rôles séparés pour chacun »

Comment ça fonctionne

Un rôle est l'unité centrale du contrôle d'accès dans GCXONE. Chaque rôle combine trois éléments :

Informations sur les rôles et utilisateurs : Détails de base du rôle (nom, description, bascule de rôle par défaut) et les utilisateurs assignés à ce rôle.

Privilèges des modules : Quels modules de plateforme les utilisateurs peuvent accéder, et quelles fonctionnalités spécifiques sont activées dans chacun. Les privilèges déterminent CE qu'un utilisateur peut faire.

Attribution des entités : Quels clients, sites, appareils et capteurs peuvent être accessibles par les utilisateurs. L'accès à l'entité détermine OÙ un utilisateur peut opérer. Les affectations d'entités peuvent être configurées à deux niveaux :

- Entités au niveau du rôle : Entités assignées au sein du rôle lui-même, partagées par tous les utilisateurs du rôle
- Entités au niveau utilisateur : Entités attribuées à des utilisateurs individuels via l'Édition de l'Accès à l'Entité, permettant à différents utilisateurs du même rôle d'accéder à différents clients ou sites

> Tip
>
> Auparavant, si deux utilisateurs avaient besoin des mêmes privilèges (par exemple, l'accès Admin) mais géraient des clients différents, il fallait créer deux rôles distincts. Maintenant, créez un seul rôle et personnalisez l'accès à l'entité par utilisateur via Modifier l'accès à l'entité.

Hiérarchie des entités

GCXONE organise les entités selon une structure hiérarchique. Le Fournisseur de Service est le compte de premier niveau (votre locataire), et toutes les entités sont imbriquées en dessous : Fournisseur de services → Client → Site → Dispositif → Capteur.

Sélection en cascade : La sélection d'un client inclut automatiquement tous les sites, appareils et capteurs en dessous. Cela garantit que de nouvelles entités sont automatiquement incluses lors de l'utilisation de l'option Inclure des enfants et simplifie la configuration.

Résolution des autorisations : Lorsqu'un utilisateur a plusieurs rôles (affectations directes + appartenance à des groupes), tous les privilèges se combinent de manière additive. Les changements entrent en vigueur en 5 secondes sur les plateformes web et mobiles.

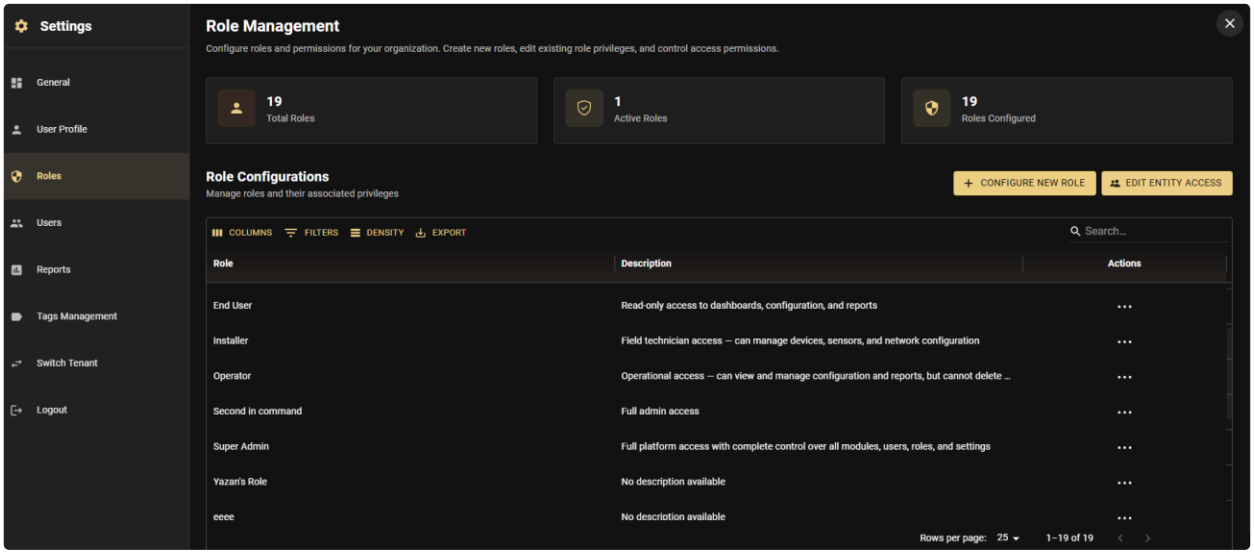
Capacités clés

Rôles par défaut

GCXONE inclut des rôles préconfigurés pour vous aider à démarrer rapidement. Chaque rôle est accompagné d'un ensemble défini de privilèges de module. L'accès à l'entité peut être personnalisé par utilisateur.

- Super Admin — Accès complet à la plateforme avec contrôle total sur tous les modules, utilisateurs, rôles et réglages. Accès administratif complet à toutes les fonctionnalités du système. Peut gérer tous les utilisateurs, rôles et permissions. Accès complet à toutes les entités. Configurez les paramètres à l'échelle du système et les journaux d'audit. Un Super Admin par locataire. Ne peut pas être supprimé.
- Administration — Accès administratif — peut gérer les utilisateurs, les rôles, la configuration et les rapports, mais pas la facturation. Gérer les utilisateurs et l'attribution des rôles. Configurez les paramètres système. Créer et gérer des groupes d'entités. Consultez les journaux d'audit et les rapports. Impossible d'accéder à la facturation. Impossible de supprimer les composants critiques du système.

- Opérateur — Accès opérationnel — peut consulter et gérer la configuration et les rapports mais ne peut pas supprimer ni administrer les utilisateurs/rôles. Surveillance quotidienne et traitement des alarmes. Consultez les tableaux de bord et la configuration. Générez et consultez des rapports. Gérer les tâches opérationnelles. Impossible de supprimer les composants système. Capacités administratives limitées.
- Installateur — Accès des techniciens de terrain — peut gérer les appareils, capteurs et la configuration réseau. Gérer les dispositifs physiques et les capteurs. Configurez les paramètres réseau. Installer et configurer le matériel. Dépanner les problèmes de périphérique. Impossible de gérer les utilisateurs ou les rôles.
- Utilisateur final — Accès en lecture seule aux tableaux de bord, configuration et rapports. Consultez les tableaux de bord et la configuration de base. Accédez aux rapports de base. Consultez les caméras et appareils assignés. Armer/désarmer pour les dispositifs/sites assignés. Aucune possibilité de modifier les paramètres ou d'administrer le système.



Vous pouvez utiliser ces rôles par défaut tels quels, les personnaliser ou créer de nouveaux rôles à partir de zéro.

Privilèges des modules

Les privilèges sont organisés par module de plateforme. Chaque module dispose d'un interrupteur d'accès à la page et de paramètres de capacités granulaires. Les privilèges déterminent QUELLES actions un utilisateur peut effectuer sur la plateforme.

- Tableau de bord — Bascule de page d'accès, filtre comptes, filtre de capacités
- Perspectives de gestion — Activer le rôle, modifier le rôle et des capacités analytiques supplémentaires
- Configuration — Utilisateurs mobiles, rôles, sous-analyses, bilan de santé, groupes clients, table de capteurs, audits, tableau des concessionnaires, tableau des fournisseurs de services, IoT, tableau groupe/stade, groupe client, fournisseur de services, client, site, tableau de bord de configuration
- Recherche d'activité vidéo — Édition sauvegardée, Utiliser le filtre, Live, Lecture, Filtre d'édition, Filtre d'alarme
- Marché — Vue impulsion, rôles, synchronisation temporelle, contrôle de santé, compte du minuteur, mode Zen, importation en masse
- Visualiseur vidéo — Contrôles vidéo, bascules de capacité
- Gestionnaire d'alarme — Contrôles vidéo, bascules de capacité
- Carte — Modifier la carte, ajouter un capteur, ajouter des entrées /s, modifier les sorties, gérer la révision, gérer les sorties, vidéo en direct, vue en direct, moniteur mural, voir le tableau de bord

Chaque module dispose d'une option Sélectionner Tout / Supprimer Tout pour une configuration rapide en bloc, ainsi qu'un bouton d'accès à la page qui active ou désactive l'ensemble du module.

Accès à l'Entité : Trois modes

Lors de la configuration de l'accès à l'entité lors de la création (ou de l'édition de rôle), trois modes sont disponibles. L'accès à l'entité détermine OÙ un utilisateur peut opérer — il contrôle quels clients, sites, appareils et capteurs sont visibles et accessibles à l'utilisateur.

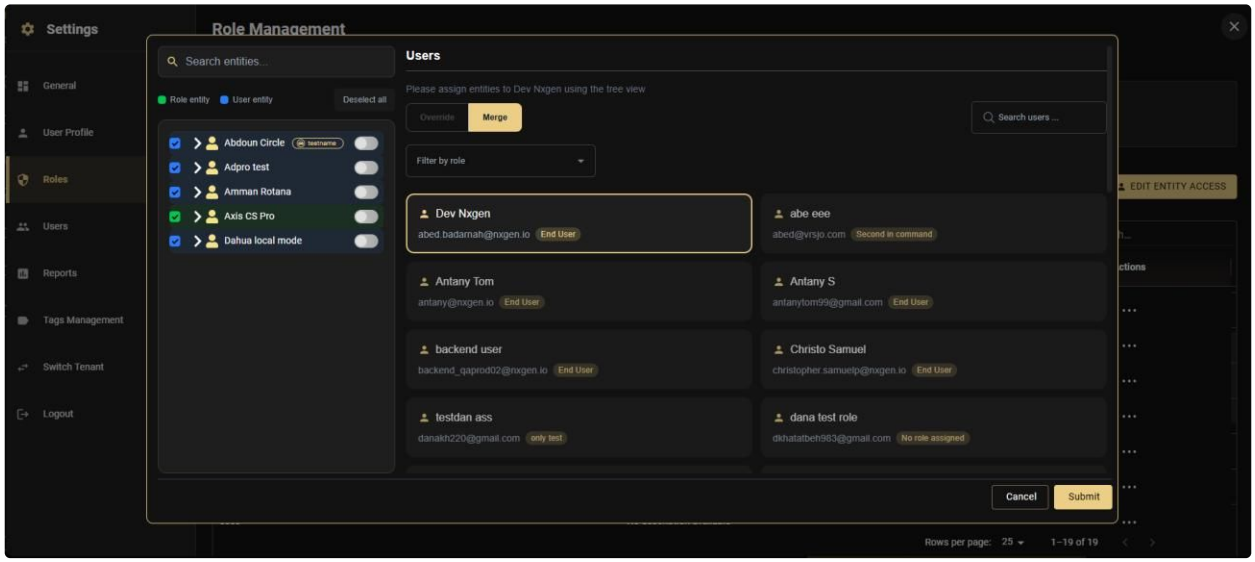
- Aucun accès à l'entité — Les utilisateurs n'ont aucun accès à l'entité par défaut. Doit être attribué par utilisateur via Modifier l'Accès à l'Entité. Optimal pour : Rôle partagé avec chaque entité assignée.
- Entités sélectionnées — Les utilisateurs sont limités aux entités spécifiquement sélectionnées (avec ou sans enfants). Idéal pour : Sous-listes spécifiques ou locataires avec un accès identique.
- Accès complet — Les utilisateurs passent par défaut à l'accès complet pour tous les clients, sites, appareils et capteurs. Idéal pour : les postes d'administrateur ou de super-utilisateur nécessitant un accès illimité.

Quel que soit le mode : Vous pouvez toujours personnaliser la liste d'entités pour des utilisateurs spécifiques via Modifier l'Accès à l'Entité, en supplantant ou en prolongeant les attributions au niveau du rôle tout en conservant leurs privilèges de rôle.

Le bouton Inclure des enfants : Lors de la sélection d'entités dans la vue arborescente, chaque entité dispose d'un bascule Inclure des enfants (affiché par un curseur bleu à côté du nom de l'entité). Ce bouton a un impact crucial sur le fonctionnement de l'accès :

Sans inclure les enfants : Seules les entités sélectionnées manuellement sont incluses. Si vous sélectionnez le Site A et ses 5 appareils et 30 capteurs individuellement, l'utilisateur a accès exactement à ces éléments. Les futurs appareils ou capteurs ajoutés sous ce site ne seront PAS automatiquement inclus — il faudrait revenir manuellement à Modifier l'accès à l'entité et sélectionner le nouvel appareil.

Avec inclure des enfants : Il suffit de sélectionner l'entité mère (par exemple, Site A). Tous les appareils et capteurs en dessous sont automatiquement inclus. Tous les futurs appareils ou capteurs ajoutés sous ce site sont automatiquement inclus — aucune mise à jour manuelle n'est nécessaire.



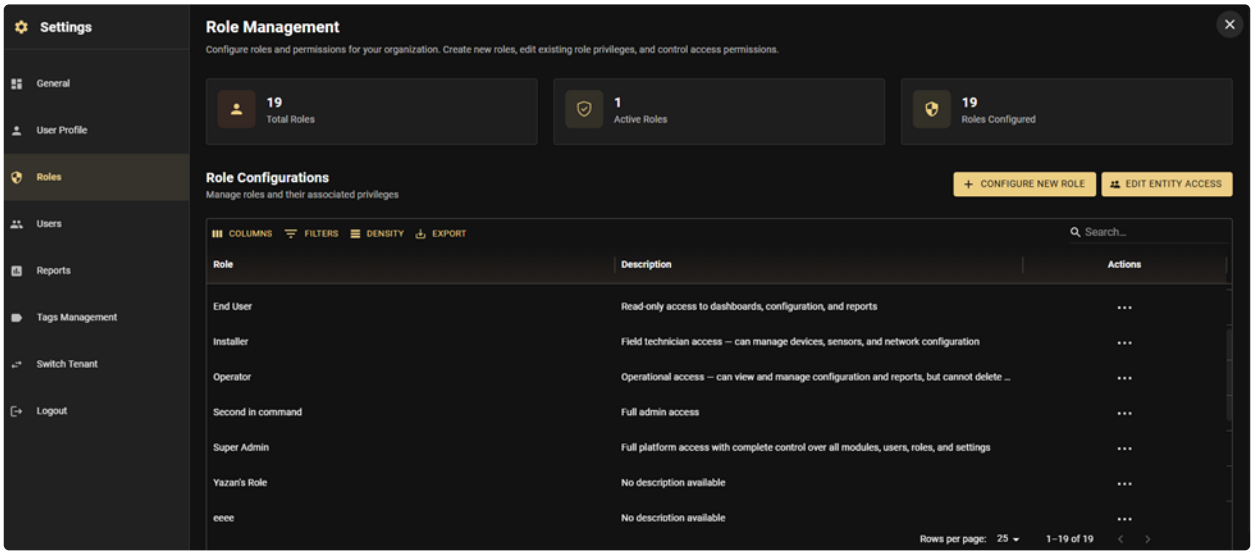
> Tip
>
> Utilisez Inclure les enfants autant que possible. Cela permet de gagner du temps et garantit que les nouveaux appareils sont automatiquement accessibles aux bons utilisateurs. N'utilisez la sélection manuelle que lorsque vous devez spécifiquement restreindre l'accès à un ensemble fixe d'entités.

Fonctions de gestion

Navigation : Paramètres → rôles

La page Gestion des rôles affiche tous les rôles configurés avec leurs descriptions et propose deux boutons d'action principaux :

- Configurer un nouveau rôle — Ouvre le magicien de création de rôles guidé
- Modifier l'accès à l'entité — Ouvre l'interface de gestion d'accès par entité



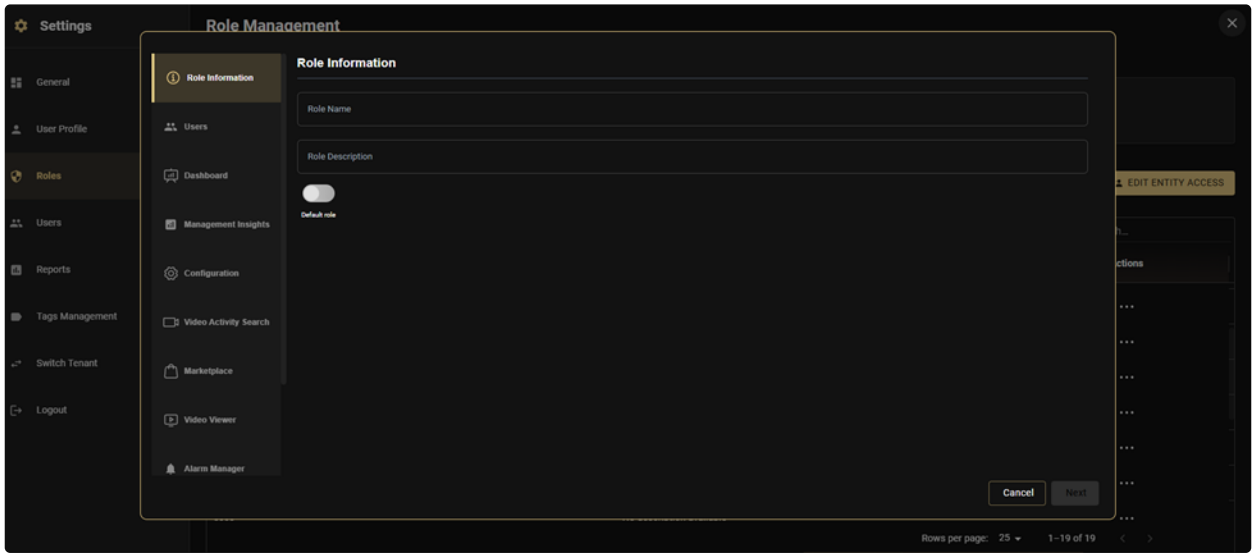
Créer un rôle

Navigation : Paramètres → rôles → Configurer un nouveau rôle

L'assistant de création de rôle vous guide à travers un processus en plusieurs étapes. Chaque étape est accessible via son onglet dans la barre latérale gauche.

Étape 1 : Informations sur le poste

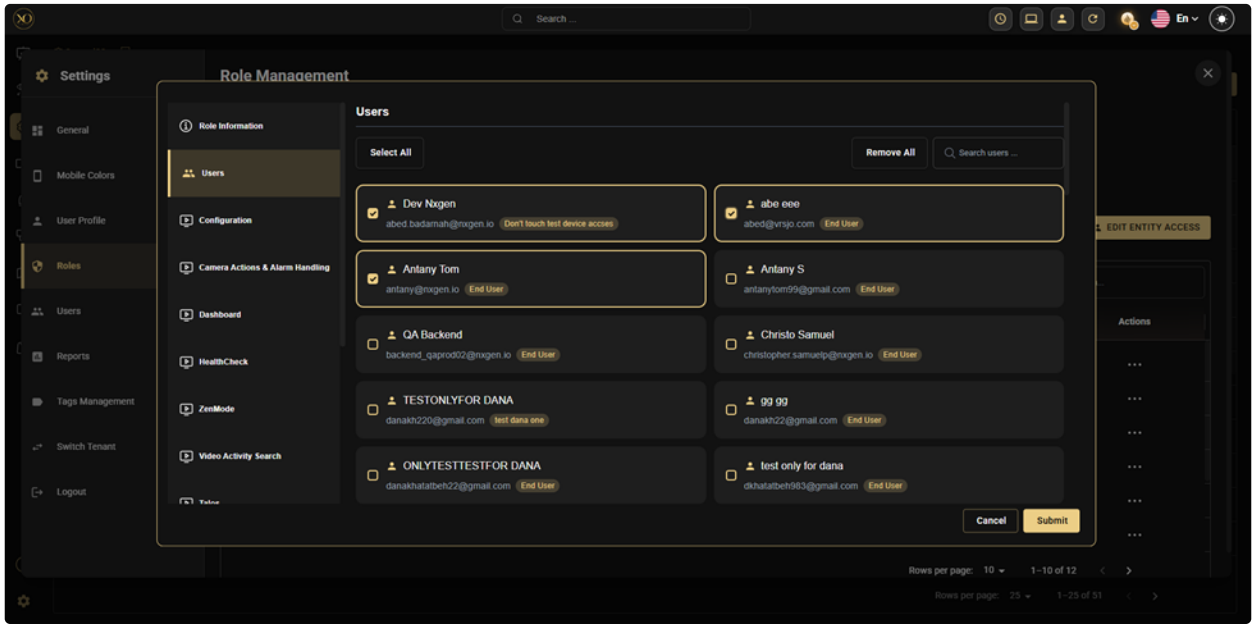
1. Nom du poste — Un nom unique identifiant le rôle (par exemple, « Administrateur régional », « Opérateur uniquement en vue »)
2. Description du rôle — Une brève description de la raison d'être du poste
3. Bascule de rôle par défaut — Une fois activé, ce rôle sera automatiquement attribué aux nouveaux utilisateurs lorsqu'ils sont invités sur la plateforme. C'est utile pour des rôles de base comme « Utilisateur final » que chaque nouveau membre de l'équipe devrait adopter.



La première étape de la gestion des rôles, demandant un nom et une description de rôle, avec un interrupteur pour en faire le rôle par défaut.

Étape 2 : Utilisateurs

Sélectionnez quels utilisateurs doivent être assignés à ce rôle. L'étape des utilisateurs affiche tous les utilisateurs disponibles dans une grille consultable avec leurs badges de rôle actuels. Cliquez sur une carte utilisateur pour la sélectionner (surlignée d'une bordure dorée). Utilisez Sélectionner Tout, Supprimer Tout ou Rechercher Utilisateurs pour la gestion en masse.

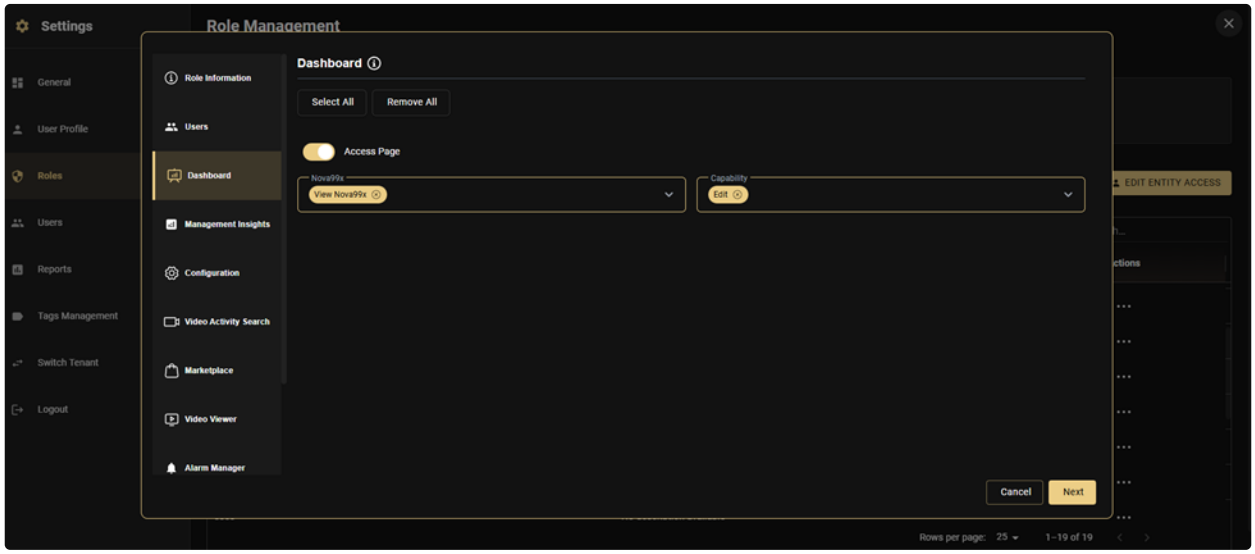


Étape 3 : Privilèges du module

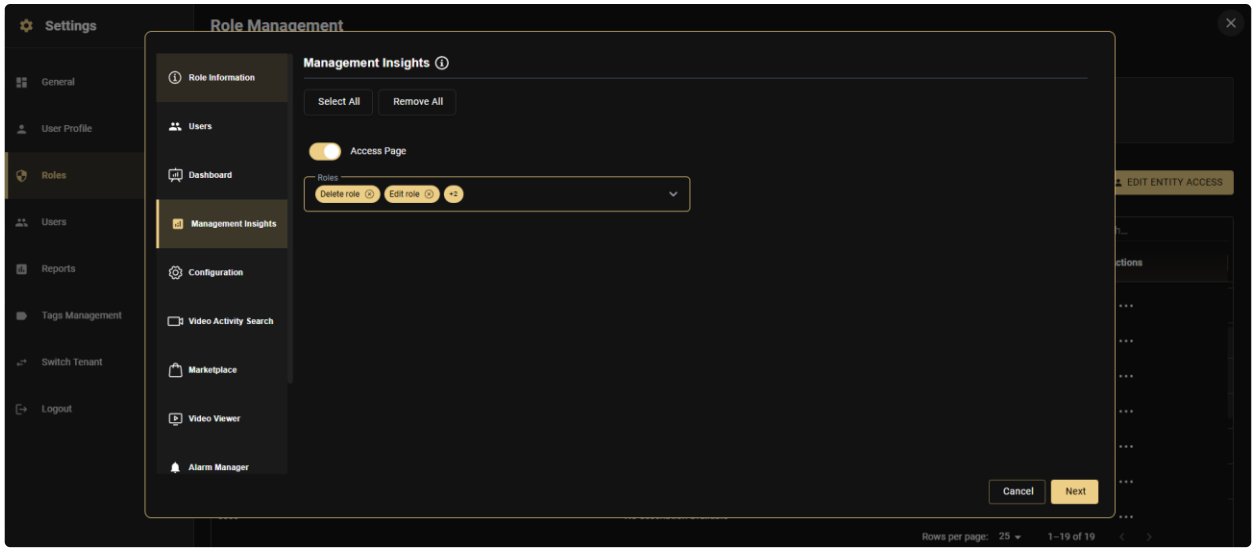
Configurez l'accès pour chaque module de plateforme. L'assistant présente chaque module sous forme d'onglet séparé dans la barre latérale. Pour chaque module :

1. Activez/désactivez la page d'accès pour activer ou désactiver l'ensemble du module
2. Utilisez Sélectionner Tout / Supprimer Tout pour une sélection rapide en masse des fonctionnalités
3. Sélectionnez les capacités individuelles dans les menus déroulants pour affiner l'accès

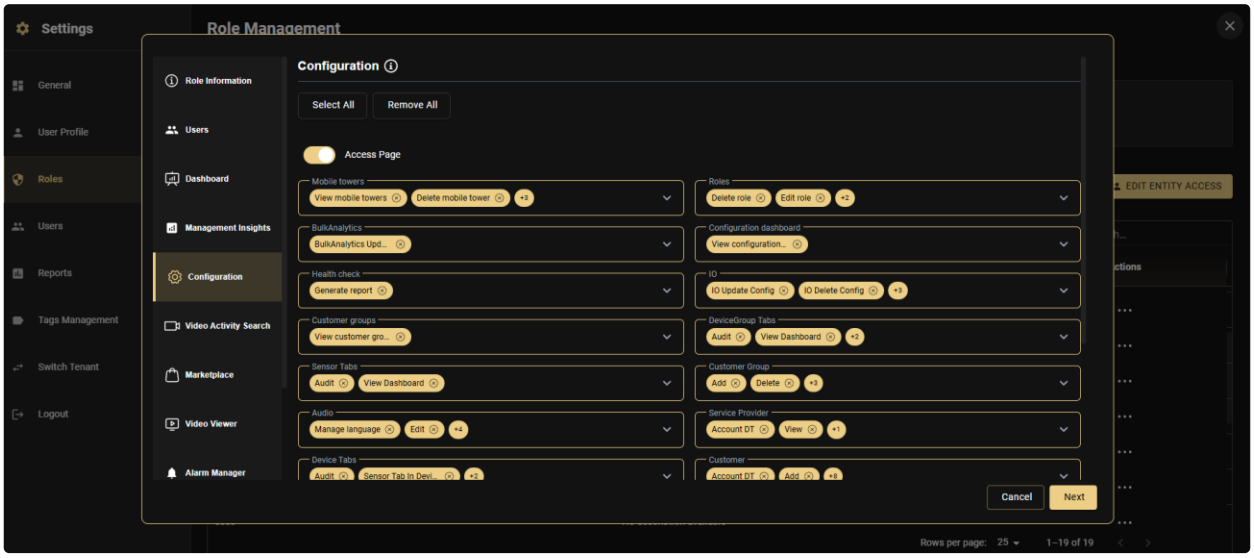
Tableau de bord :



Analyses de gestion :

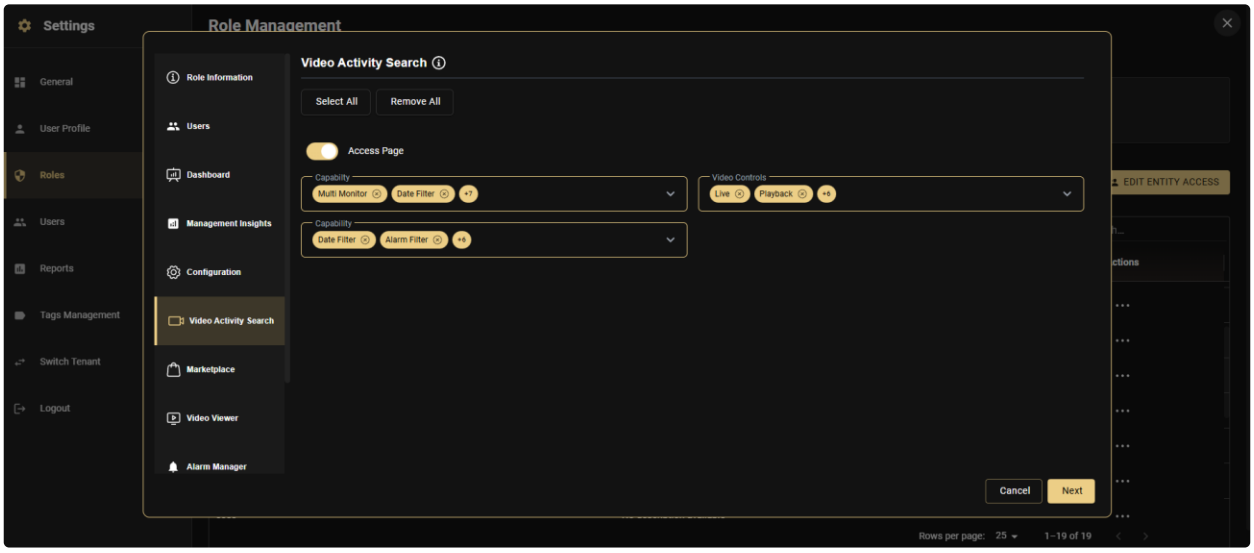


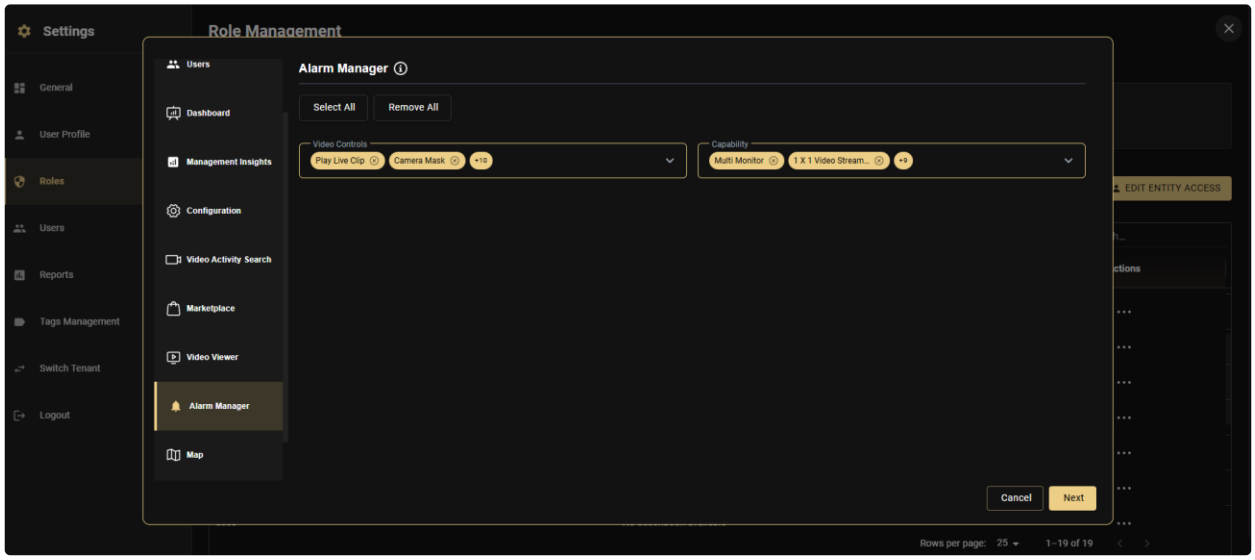
Configuration :



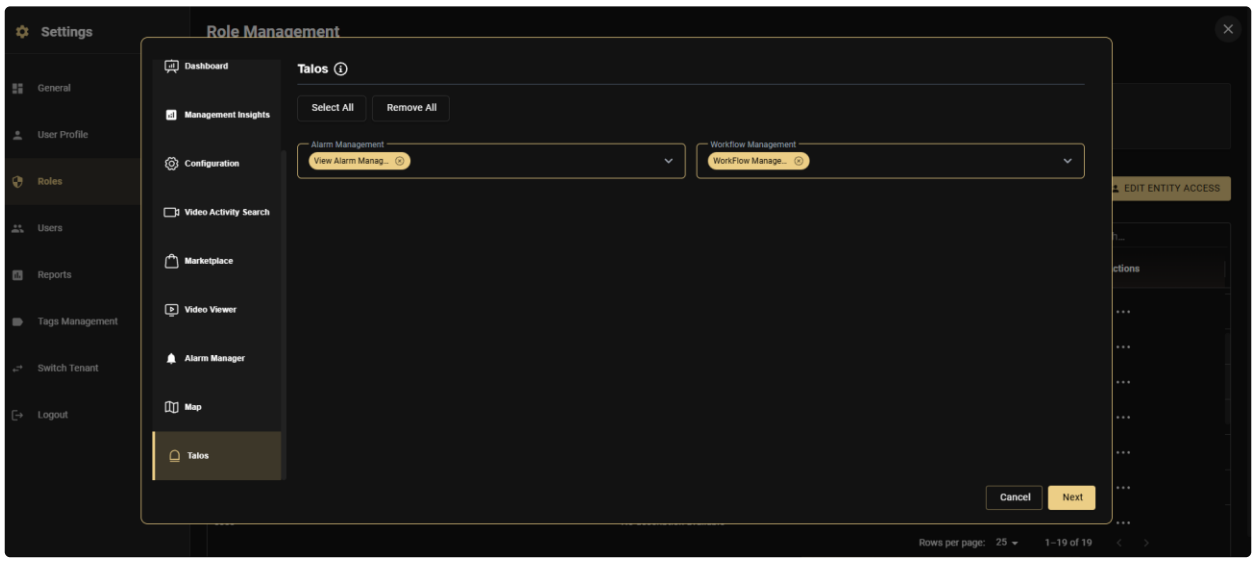
L'étape Configuration de la gestion des rôles, où chaque domaine — tours mobiles, analytique, contrôle d'état, capteurs, audio, appareils, rôles et autres — reçoit son propre jeu d'autorisations.

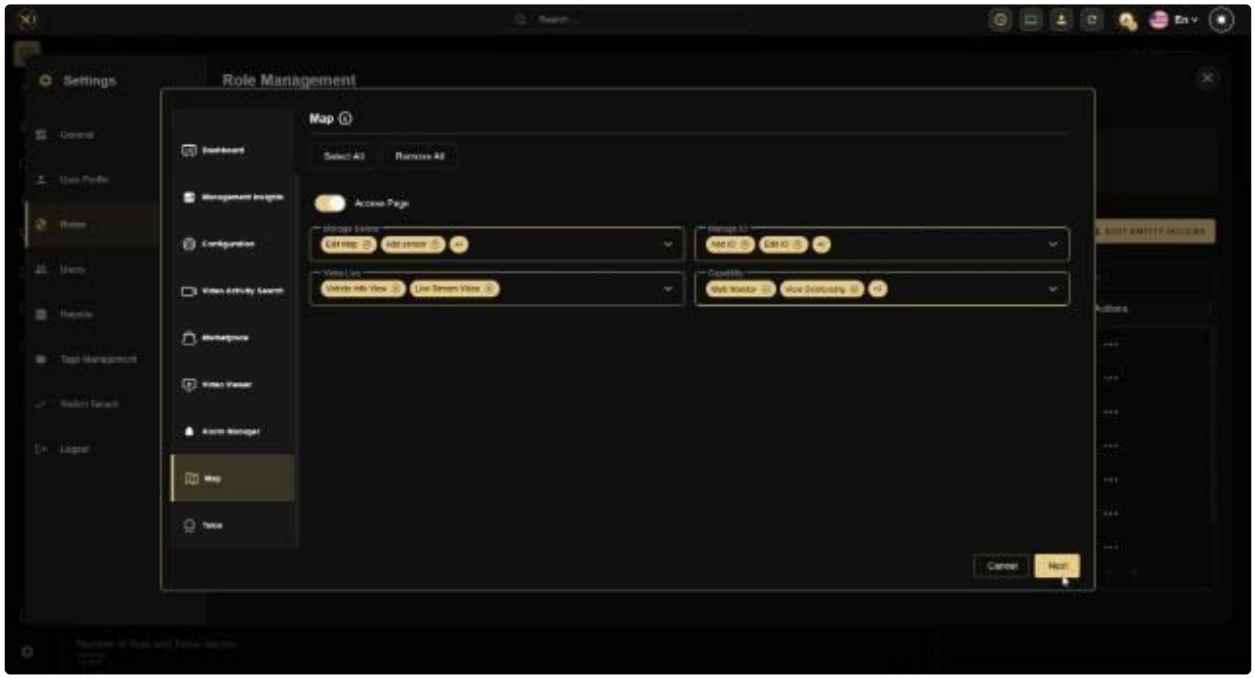
Recherche d’activité vidéo :



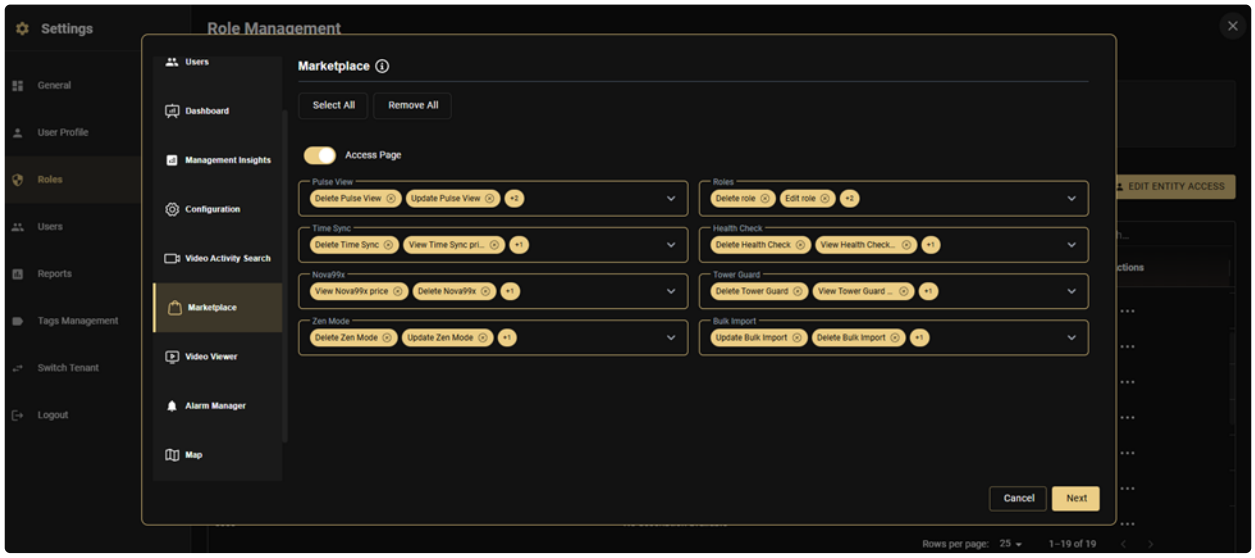


Gestionnaire d'alarme :

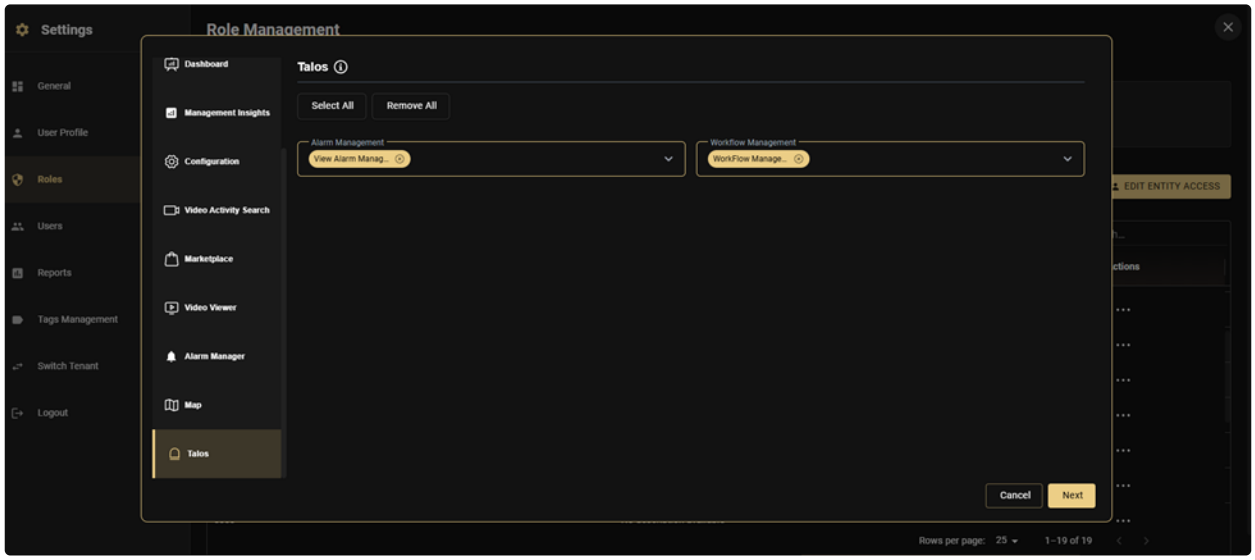




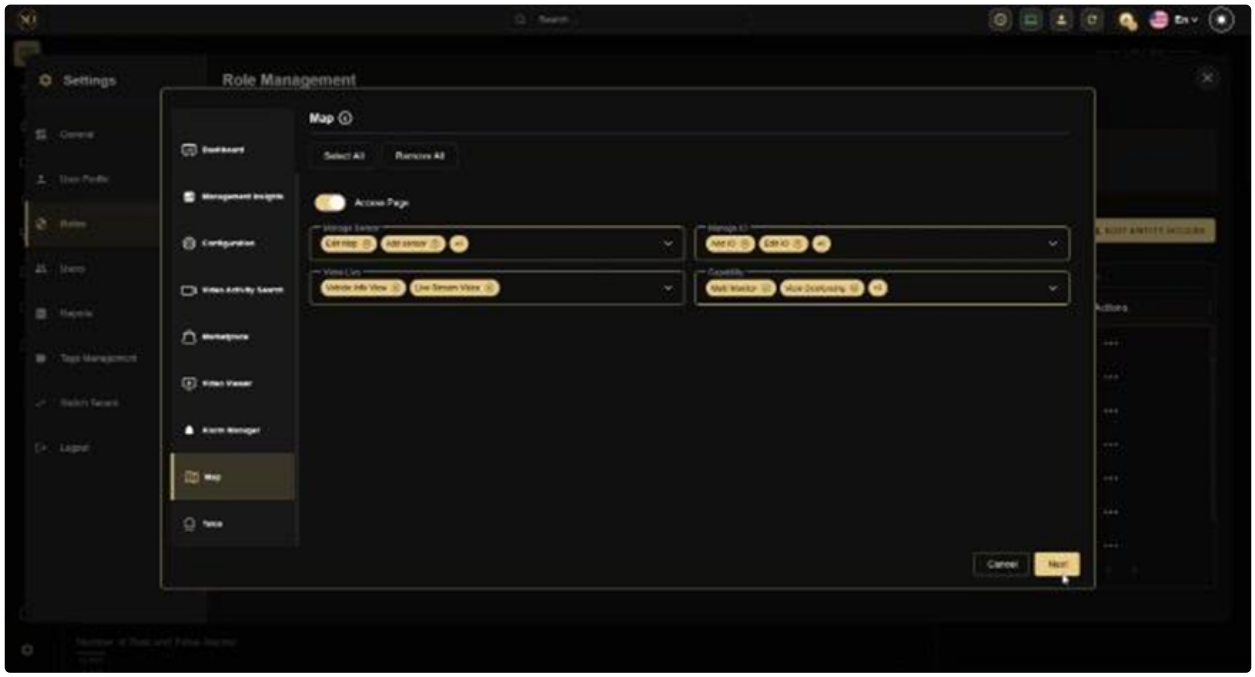
Marché :



Talos :



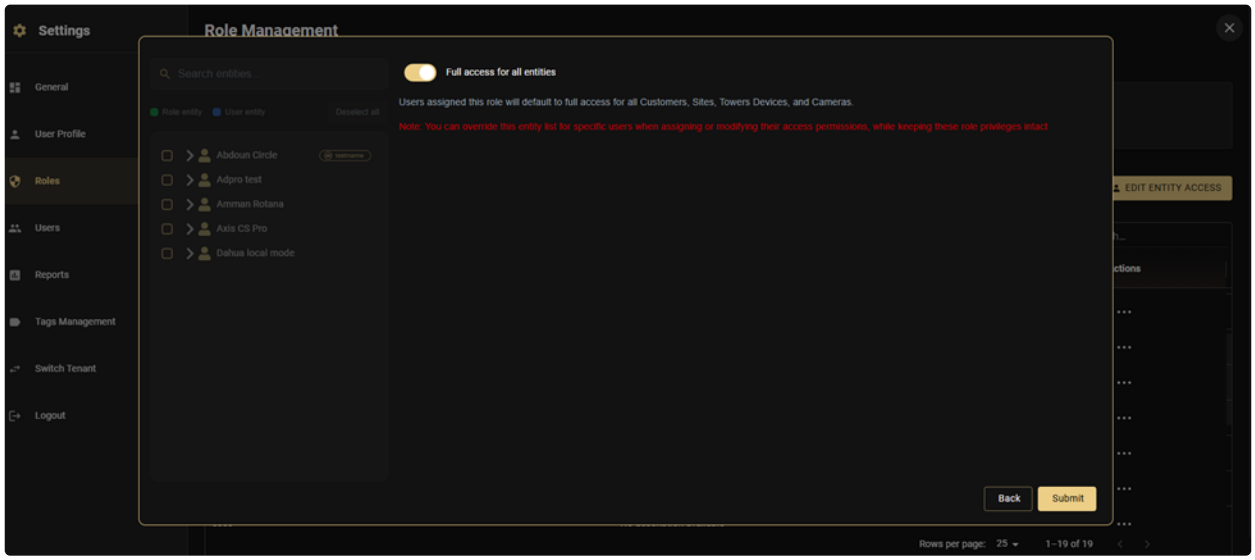
Carte :



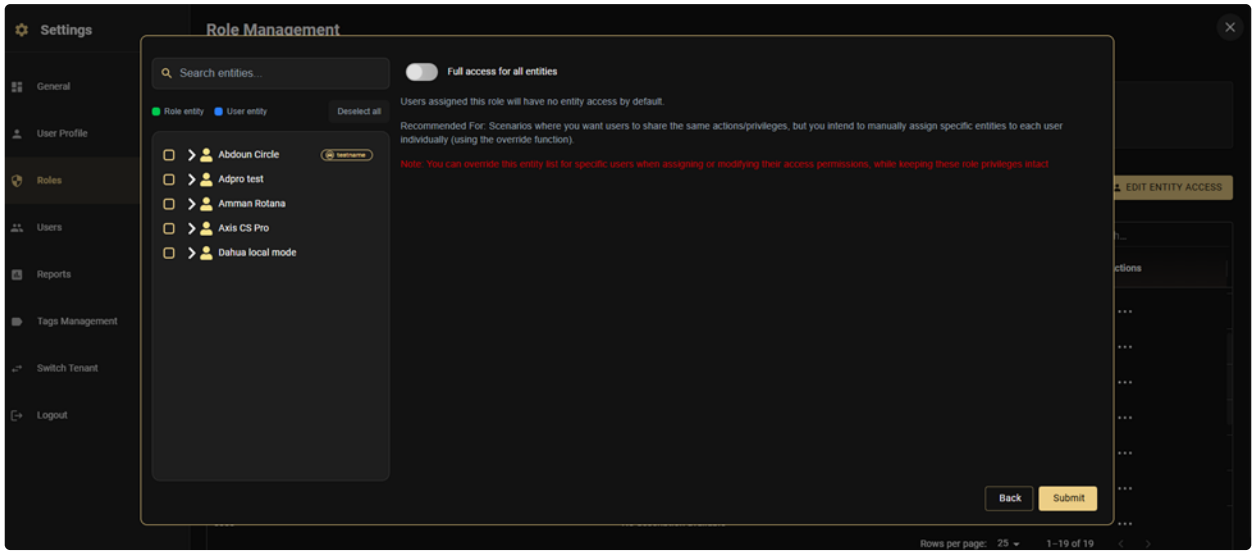
Étape 4 : Attribution d'entités

La dernière étape consiste à définir quelles entités les utilisateurs de ce rôle peuvent accéder. L'arbre d'entités est affiché sur le côté gauche avec des cases à cocher pour la sélection et les options Inclure les enfants pour chaque entité.

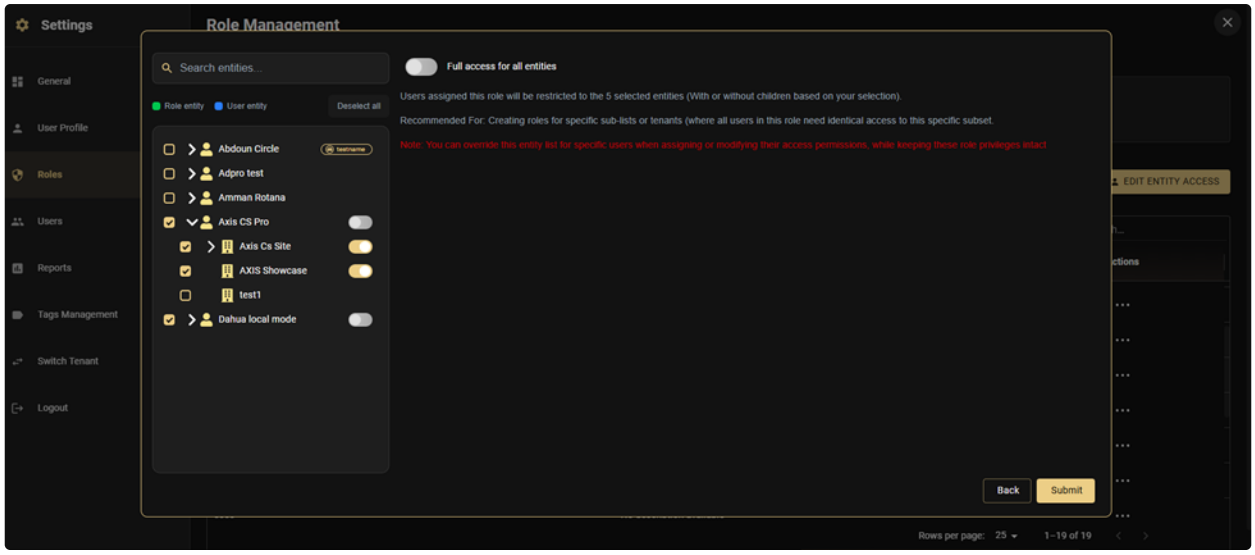
Accès complet pour toutes les entités (activer la mise en marche) : Les utilisateurs assignés à ce rôle auront par défaut un accès complet pour tous les clients, sites, tours/appareils et caméras.



Aucun accès à l'entité (désactiver le bouton OFF, aucune unité sélectionnée) : Les utilisateurs attribués à ce rôle n'auront aucun accès à l'entité par défaut. Recommandé pour les scénarios où vous souhaitez que les utilisateurs partagent les mêmes privilèges, mais que vous souhaitez assigner manuellement des entités spécifiques à chaque utilisateur individuellement en utilisant la fonction Modifier l'accès à l'entité.



Entités sélectionnées (désactiver le bouton OFF, entités cochées) : Les utilisateurs attribués à ce rôle seront limités aux entités sélectionnées. Avec le bouton Inclure les enfants activé sur certains éléments, toutes les sous-entités (actuelles et futures) sont automatiquement incluses.



L'étape d'accès aux entités de la gestion des rôles, avec l'accès complet désactivé et des sites précis cochés dans l'arborescence, limitant le rôle aux entités sélectionnées.

Avertissement : Lors de la sélection des entités sans Inclure les enfants, seuls les éléments existants et sélectionnés manuellement sont inclus. Les nouveaux appareils ajoutés ultérieurement ne seront PAS automatiquement accessibles. Envisagez toujours d'utiliser Inclure les enfants pour assurer l'avenir de vos affectations d'entités. Exemple : Vous assignez l'utilisateur X au site A, qui possède actuellement un appareil. Si un nouvel appareil est ajouté ultérieurement sous le site A et que l'option Inclure les enfants a été désactivée, l'utilisateur X ne verra toujours que l'appareil d'origine. Il faudrait aller manuellement dans Modifier l'accès à l'entité et ajouter le nouvel appareil pour cet utilisateur.

Cliquez sur Soumettre pour créer le poste.

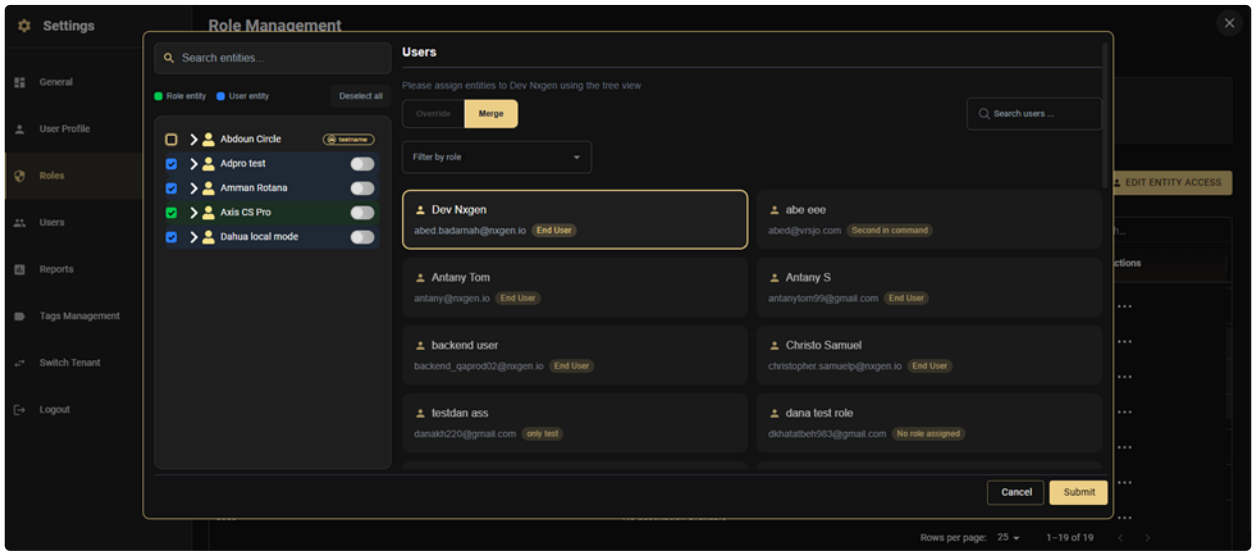
Modifier l'accès à l'entité (gestion par utilisateur)

Navigation : Paramètres → rôles → Modifier l'accès à l'entité

C’est la fonctionnalité clé qui vous permet de personnaliser l’accès à l’entité pour chaque utilisateur sans créer de rôles séparés. N’oubliez pas : l’accès à l’entité détermine OÙ un utilisateur peut opérer, pas ce qu’il peut faire. Les privilèges viennent toujours du rôle.

L’interface est divisée en deux panneaux :

- Panneau de gauche : Arbre d’entités avec les onglets Entité de rôle, Entité utilisateur et Connecté à
- Panneau de droite : Liste des utilisateurs avec des onglets de recherche, filtrage des rôles et mode Option/Fusion



L'étape Users de la gestion des rôles avec Merge sélectionné plutôt qu'Override, afin que le rôle s'ajoute aux entités déjà attribuées à chaque personne.

Comment personnaliser l’accès à l’entité d’un utilisateur

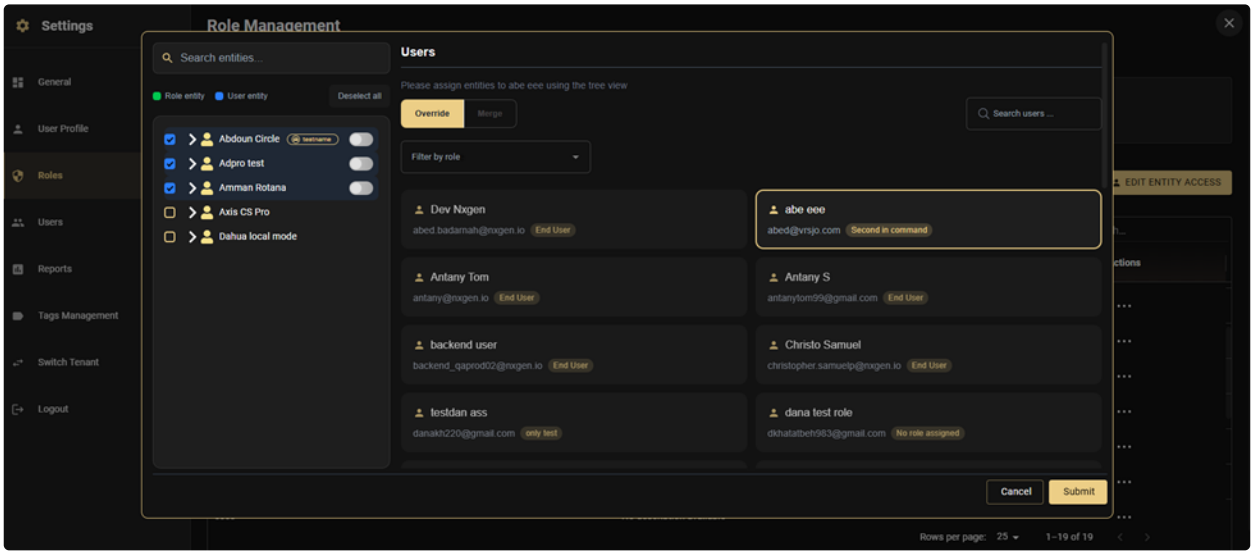
1. Cliquez sur Modifier l’accès à l’entité depuis la page Gestion des rôles
2. Sélectionnez un utilisateur depuis le panneau de droite en cliquant sur sa carte
3. Choisissez le mode : Override ou Merge
4. Utilisez l’arbre d’entités à gauche pour sélectionner ou désélectionner des entités pour cet utilisateur spécifique

5. Activez l'inclusion des enfants sur les entités où vous souhaitez inclure toutes les sous-entités actuelles et futures. C'est crucial pour garantir que toute nouvelle caméra, appareil ou capteur ajouté sous une entité mère soit automatiquement inclus dans la liste d'accès de l'entité de l'utilisateur, sans nécessiter de mises à jour manuelles. Exemple : Vous assignez l'utilisateur X au site A, qui possède actuellement un appareil. Le lendemain, un nouvel appareil est ajouté sous le Site A (maintenant 2 appareils au total). Si Inclure des enfants était désactivé pour le Site A, l'utilisateur X ne verra toujours que l'appareil original et n'aura PAS accès à celui nouvellement ajouté. Si Inclure les enfants était activé, l'utilisateur X voit automatiquement les deux appareils — aucune mise à jour manuelle n'est nécessaire.
6. Cliquez sur Soumettre pour enregistrer les modifications

Outre vs. Fusion

Mode de dérogation : La sélection personnalisée de l'entité de l'utilisateur REMPLACE les paramètres par défaut au niveau du rôle. Tout ce que vous choisissez pour cet utilisateur prime sur ce que le rôle offre. Utilisez cela lorsque vous souhaitez avoir un contrôle total sur l'accès à l'entité d'un utilisateur spécifique.

Mode de fusion : Les entités sélectionnées sont AJOUTÉES en plus des attributions existantes du poste. L'utilisateur obtient à la fois les entités au niveau du rôle ET les entités supplémentaires au niveau utilisateur. Utilisez cela pour étendre l'accès de l'utilisateur au-delà de ce que le rôle propose.



L'étape Users de la gestion des rôles, avec l'arborescence des entités à gauche et les personnes pouvant être affectées au rôle à droite, au-dessus des options Override et Merge.

Vous pouvez également filtrer la liste des utilisateurs par rôle à l'aide du menu déroulant en haut du panneau de droite, ce qui facilite la gestion de l'accès aux entités pour tous les utilisateurs d'un rôle donné.

Conseil : Utilisez le menu déroulant « Filtrer par rôle » pour trouver rapidement tous les utilisateurs assignés à un rôle spécifique et personnaliser leur accès à l'entité en masse.

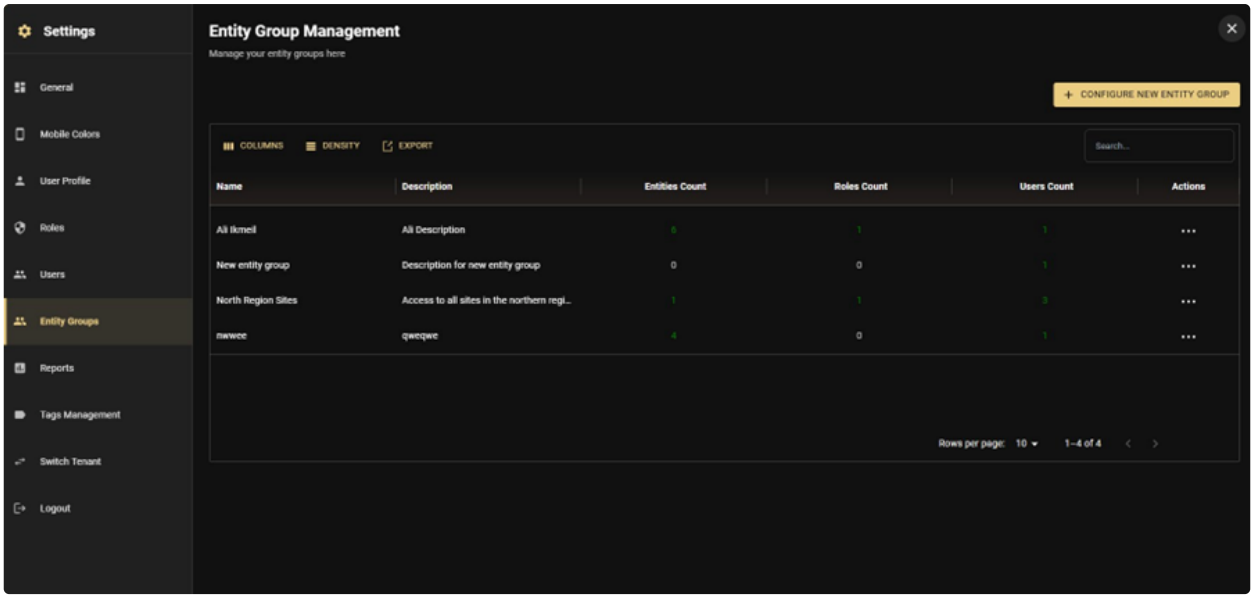
Groupes d'entités gestionnaires

Navigation : Paramètres → Groupes d'entités

Les groupes d'entités sont des collections sauvegardées et réutilisables d'entités (clients, sites, appareils et capteurs) qui servent de modèles. Au lieu de sélectionner manuellement les mêmes entités à chaque configuration d'un rôle ou d'attribution d'un accès utilisateur, vous définissez le groupe une fois et l'appliquez là où c'est nécessaire. Pensez à un groupe d'entités comme un raccourci nommé pour un ensemble spécifique d'entités.

Groupes d'entités : Définissez le groupe une fois, puis sélectionnez-le par nom lors de l'attribution d'un accès à une entité à un rôle ou un utilisateur. Tout rôle ou utilisateur attribué à ce groupe reçoit automatiquement les bonnes entités.

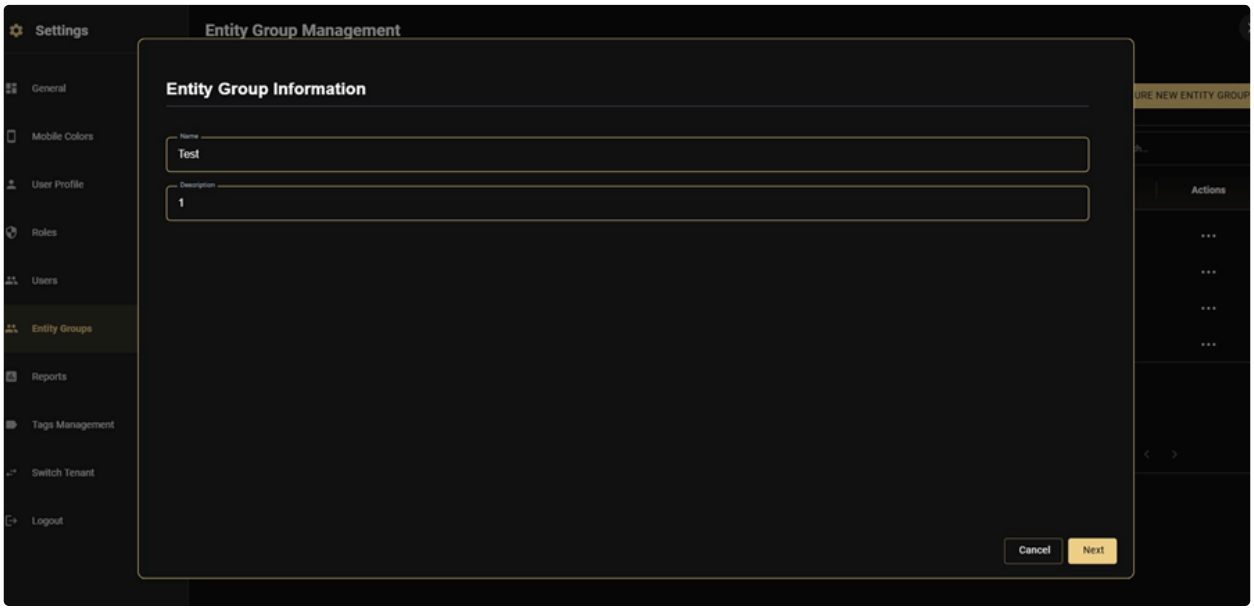
La page Groupes d'entités liste tous les groupes existants dans un tableau montrant le Nom, la Description, le Nombre d'Entités, le Nombre de Rôles et le Nombre d'Utilisateurs. À partir de là, vous pouvez rechercher, exporter et configurer de nouveaux groupes en utilisant le bouton Configurer un nouveau groupe d'entité.



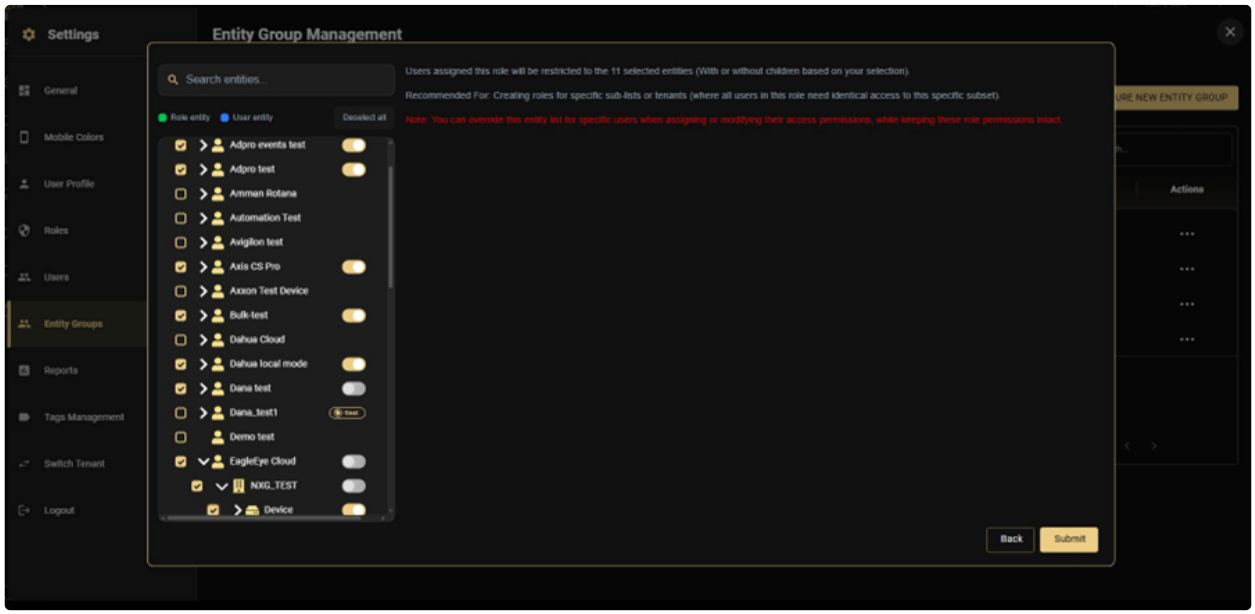
Création d'un groupe d'entités

Cliquez sur Configurer un nouveau groupe d'entité pour ouvrir l'assistant de création en deux étapes.

Étape 1 — Informations sur le groupe : Saisissez un nom et une description optionnelle pour le groupe, puis cliquez sur Suivant.

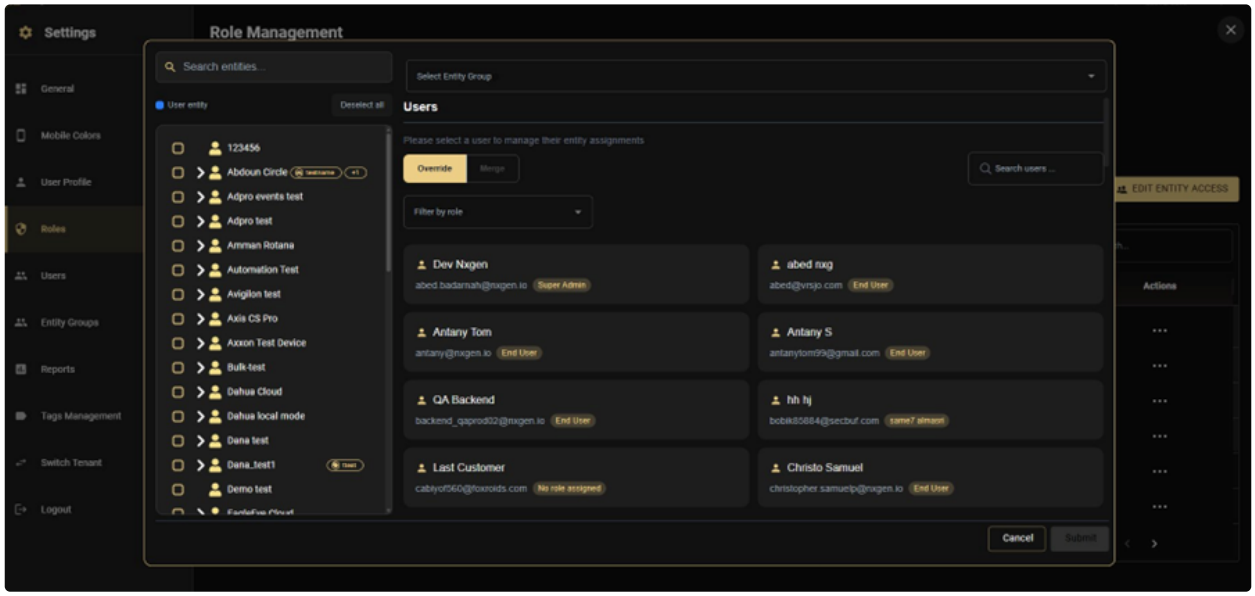


Étape 2 — Sélectionnez les entités : Utilisez l'arbre d'entités pour vérifier les clients, sites, appareils ou capteurs à inclure dans ce groupe. Utilisez l'option Inclure les enfants à côté de n'importe quelle entité pour inclure automatiquement toutes les sous-entités actuelles et futures en dessous. Un résumé à droite montre combien d'entités sont sélectionnées ainsi que quels rôles et utilisateurs sont actuellement concernés. Cliquez sur Soumettre pour sauver le groupe.



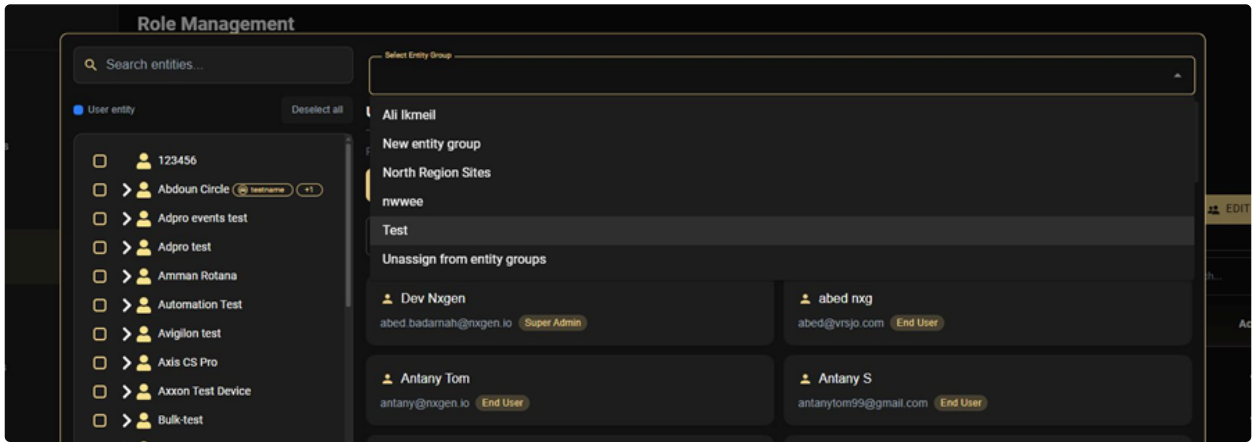
Assignation d'un groupe d'entités à un rôle ou à un utilisateur
Les groupes d'entités peuvent être appliqués en deux endroits :

- Lors de l'attribution des entités de rôle (étape 4 de la création/édition du rôle) : Dans l'écran de sélection d'entité, utilisez le menu déroulant Sélectionner le groupe d'entité pour appliquer un groupe enregistré. Toutes les entités de ce groupe sont immédiatement chargées dans la sélection. Tous les utilisateurs du rôle hériteront de ces entités.



L'étape Users de la gestion des rôles avec Override sélectionné, l'arborescence des entités à gauche et les personnes à affecter à droite, chacune étiquetée du rôle qu'elle occupe déjà.

- Dans l'Édition de l'Accès à l'Entité (par utilisateur) : Après avoir sélectionné un utilisateur dans le panneau Modifier l'Accès à l'Entité, utilisez le menu déroulant Sélectionner le groupe d'entités en haut pour charger rapidement les entités d'un groupe pour cet utilisateur. Le paramètre de mode Override ou Merge s'applique toujours — le groupe pré-remplit simplement la sélection des entités.



Conseil : Les groupes d'entités sont particulièrement utiles lorsque plusieurs rôles ou utilisateurs ont besoin d'accéder au même ensemble de sites ou de clients. Créez le groupe une fois, puis appliquez-le à autant de rôles et d'utilisateurs que nécessaire. Si la liste des entités change, mettez à jour le groupe en un seul endroit et tous les rôles et utilisateurs attribués reflètent automatiquement le changement.

Montage d'un rôle

Navigation : Paramètres → rôles → [Nom du rôle] → Modifier (via le menu Actions)

Le flux d'édition utilise la même interface d'assistant que la création de rôle. Modifiez n'importe quelle étape — informations de rôle, utilisateurs, privilèges de module ou assignations d'entités — puis enregistrez. Les changements affectent immédiatement tous les utilisateurs ayant ce rôle.

Avertissement : Supprimer l'accès aux modules ou entités peut perturber les flux de travail des utilisateurs. Vérifiez qui occupe ce poste avant d'apporter des changements significatifs.

Suppression d'un rôle

Navigation : Paramètres → rôles → [Nom du rôle] → Supprimer (via le menu Actions)

Le système avertit si des utilisateurs sont actuellement affectés au poste et liste les utilisateurs concernés. Les rôles système (Admin, Super Admin) ne peuvent pas être supprimés.

Bonnes pratiques

Exemple 1 : Deux administrateurs régionaux, un seul poste

Scénario : Vous avez deux administrateurs régionaux qui ont besoin de privilèges identiques (surveillance complète, contrôle des alarmes, exportation vidéo), mais l'administrateur A gère les clients du Nord-Est tandis que l'Administrateur B gère ceux du Sud-Est. Auparavant, cela nécessitait deux rôles distincts. Maintenant, il ne vous en faut qu'un.

Étape 1 — Créer le rôle sans accès par défaut à l'entité :

1. Va dans Paramètres → rôles → configure un nouveau rôle
2. Informations sur le rôle : Nom = « Administrateur régional », Description = « Surveillance complète et contrôle d'alarme pour la région assignée »
3. Utilisateurs : Sélectionnez à la fois Admin A et Admin B dans la grille utilisateur

4. Privilèges du module : Activer le tableau de bord, le visualiseur vidéo, le gestionnaire d'alarmes, la carte avec les fonctionnalités souhaitées
5. Attribution d'entités : Laissez « Accès complet pour toutes les entités » DÉSACTIVÉ et ne sélectionnez aucune entité. Cliquez sur Envoyer.

Étape 2 — Attribuer l'accès à une entité par utilisateur :

- Va dans Paramètres → Rôles → Modifier l'accès à l'entité
- Sélectionnez Admin A → Choisir Fusionner → Vérifier tous les clients du Nord-Est (avec Inclure les enfants activé) → Soumettre
- Sélectionnez Admin B → Choisir Fusionner → Vérifier tous les clients Southeast (avec Inclure les enfants activé) → Soumettre

Résultat : Les deux administrateurs partagent exactement le même rôle et les mêmes privilèges, mais l'administrateur A ne voit que les clients du Nord-Est tandis que l'Administrateur B ne voit que ceux du Sud-Est. Un seul rôle au lieu de deux. Lorsque de nouveaux sites ou appareils sont ajoutés sous leurs clients assignés, ils sont automatiquement inclus grâce à Inclure les enfants.

Exemple 2 : Opérateur à vue seule

Scénario : Des opérateurs qui ne devraient regarder les caméras que pendant leur service — pas d'exportation vidéo, pas de contrôle d'alarme, juste un visionnage en direct et une lecture pour des sites spécifiques.

Configuration :

- Paramètres → rôles → Configurer un nouveau rôle
- Informations sur le rôle : Nom = « Opérateur uniquement en vue »
- Utilisateurs : Sélectionnez les opérateurs qui ont besoin de ce rôle

- Privilèges du module : Activez uniquement le tableau de bord (vue uniquement) et le visualiseur vidéo (avec vue en direct et lecture). Laissez tous les autres modules désactivés.
- Attribution d'entité : Sélectionnez des sites spécifiques que ces opérateurs couvrent dans l'arbre d'entités avec Inclure les enfants activé

Les opérateurs peuvent surveiller les caméras mais ne peuvent pas exporter les images, accéder à la configuration ou contrôler les alarmes. Parfait pour le personnel débutant ou les services de surveillance tiers.

Exemple 3 : Installateur avec accès spécifique au site

Scénario : Un installateur de terrain a besoin d'accéder à un site client spécifique pour gérer les appareils et configurer les capteurs. Ils ne devraient voir que les entités pertinentes à leur affectation actuelle.

Configuration :

- Créer un rôle « Installateur » (ou utiliser le rôle d'Installateur par défaut)
- Privilèges du module : Activer la configuration (appareils, capteurs, paramètres réseau), Visualiseur vidéo (Vue en direct pour les tests)
- Attribution d'entité : Aucun accès par défaut à l'entité
- Modifier l'accès à l'entité : Sélectionnez l'utilisateur de l'installateur → Fusionner → Sélectionnez uniquement le site spécifique sur lequel il travaille avec Inclure les enfants activé

L'installateur ne peut voir et gérer que le site spécifique ainsi que tous ses appareils/capteurs. Lorsqu'un nouvel appareil est installé sur ce site, il est automatiquement accessible. Une fois le travail terminé, retirez leur accès à l'entité ou réaffectez-les au site suivant.

Exemple 4 : Accès aux applications mobiles pour les techniciens de terrain

Scénario : Les techniciens de terrain ont besoin d'accéder à une application mobile aux sites qu'ils desservent, avec visualisation par caméra et contrôle d'alarme.

Configuration :

- Créer un rôle « Technicien de terrain » via l'assistant de rôle
- Privilèges du module : Activer le visualiseur vidéo (vue en direct), le gestionnaire d'alarme (activer/désamorcer), la carte (vue en direct)
- Attribution d'entité : Aucun accès par défaut à l'entité. Utilisez Modifier l'accès à l'entité pour attribuer à chaque technicien sa zone de service avec Inclure les enfants activé.

Comportement de l'application mobile : Le technicien se connecte à l'application mobile GCXONE et ne voit que ses sites assignés individuellement. Ils peuvent regarder les caméras en direct et armer/désarmer depuis leur téléphone. Les changements d'autorisation s'appliquent sur mobile dans les 5 secondes. Pas besoin de gérer les permissions mobiles séparément ou de créer des rôles individuels.

Ressources connexes

- Pour comprendre la hiérarchie des entités, voir Organisation & Mise en place de la hiérarchie
- Pour gérer les utilisateurs, voir Gestion des utilisateurs
- Pour comprendre les journaux d'audit, consultez Audit
- Pour contacter le support, consultez Contactez le support